CLAIMS

What is claimed is:

1. An apparatus comprising:

a processor having a normal execution mode and a secure execution environment to create a secure execution environment; and

a secure virtual machine monitor (SVMM) to implement the secure execution mode in which a plurality of separate virtual machines are created that operate simultaneously and separately from one another including at least a first virtual machine to implement trusted guest software in a protected memory area and a second virtual machine to implement a non-trusted guest operating system (OS) in a non-protected memory area;

wherein responsive to a command to tear down the secure execution environment, the SVMM causes the processor to exit out of the secure execution mode, tears down the secure execution environment, and instructs the non-trusted guest OS to resume control in the normal execution mode.

2. The apparatus of claim 1, further comprising a virtual machine control structure (VCMS) to store guest state information related to the non-trusted guest operating system (OS) for use in restoring the non-trusted guest OS in the normal execution mode.

3. The apparatus of claim 2, wherein the virtual machine control structure (VCMS) stores a guest OS entry point field to point to a command used for instructing the non-trusted guest OS to resume control at a virtual address and a host entry point field to point to a command to instruct the processor to exit out of a virtual machine execution mode.

4. The apparatus of claim 1, further comprising, the SVMM scrubbing the protected memory associated with the trusted guest software when the secure execution environment is torn down.

5. The apparatus of claim 4, further comprising, the SVMM causing the processor to exit out of a virtual machine extension mode before exiting out of the secure execution mode when the secure execution environment is torn down.

6. The apparatus of claim 1, wherein the non-trusted guest operating system (OS) issues the command to tear down the secure execution environment.

7. The apparatus of claim 1, wherein the secure virtual machine monitor (SVMM) issues the command to tear down the secure execution environment.

8. The apparatus of claim 7, wherein the secure virtual machine monitor (SVMM) issues the command to tear down the secure execution environment due to a detected security breach.

9. A method comprising:

providing a normal execution mode in a processor and a secure execution mode in a processor; and

creating a secure execution environment in which a plurality of separate virtual machines operate simultaneously and separately from one another including at least a first virtual machine to implement trusted guest software in a protected memory area and a second virtual machine to implement a non-trusted guest operating system (OS) in a non-protected memory area;

wherein responsive to a command to tear down the secure execution environment, exiting out of the secure execution mode, tearing down the secure execution environment, and instructing the non-trusted guest OS to resume control in the normal execution mode.

10. The method of claim 9, further comprising storing guest state information related to the non-trusted guest operating system (OS) for use in restoring the non-trusted guest OS in the normal execution mode.

11. The method of claim 10, further comprising:

storing a guest OS entry point field to point to a command used for instructing the guest OS to resume control at a virtual address; and

storing a host entry point field to point to a command to instruct the processor to exit out of a virtual machine execution mode.

12. The method of claim 9, further comprising scrubbing the protected memory associated with the trusted guest software when the secure execution environment is torn down.

13. The method of claim 12, further comprising causing the processor to exit out of a virtual machine extension mode before exiting out of the secure execution mode when the secure execution environment is torn down.

14. The method of claim 9, wherein the non-trusted guest operating system (OS) issues the command to tear down the secure execution environment.

15. The method of claim 9, further comprising issuing the command to tear down the secure execution environment due to a detected security breach.

16. A machine-readable medium having stored thereon instructions, which when executed by a machine, cause the machine to perform the following operations comprising:

providing a normal execution mode in a processor and a secure execution mode in a processor; and

creating a secure execution environment in which a plurality of separate virtual machines that operate simultaneously and separately from one another including at least a first virtual machine to implement trusted guest software in a protected memory area and a second virtual machine to implement a non-trusted guest operating system (OS) in a non-protected memory area;

wherein responsive to a command to tear down the secure execution environment, exiting out of the secure execution mode, tearing down the secure execution environment, and instructing the non-trusted guest OS to resume control in the normal execution mode.

17. The machine-readable medium of claim 16, wherein the instructions cause the machine to perform further operations comprising storing guest state information related to the non-trusted guest operating system (OS) for use in restoring the non-trusted guest OS in the normal execution mode.

18. The machine-readable medium of claim 17, wherein the instructions cause the machine to perform further operations comprising:

storing a guest OS entry point field to point to a command used for instructing the guest OS to resume control at a virtual address; and

storing a host entry point field to point to a command to instruct the processor to exit out of a virtual machine execution mode.

19. The machine-readable medium of claim 16, wherein the instructions cause the machine to perform further operations comprising scrubbing the protected memory associated with the trusted guest software when the secure execution environment is torn down.

20. The machine-readable medium of claim 19, wherein the instructions cause the machine to perform further operations comprising causing the processor to exit out of a virtual machine extension mode before exiting out of the secure execution mode when the secure execution environment is torn down.

21. The machine-readable medium of claim 16, wherein the non-trusted guest operating system (OS) issues the command to tear down the secure execution environment.

22. The machine-readable medium of claim 16, wherein the instructions cause the machine to perform further operations comprising issuing the command to tear down the secure execution environment due to a detected security breach.

23. A system comprising:

a processor including virtual machine extension (VMX) instruction support, the processor further having a normal execution mode and a secure execution mode to create a secure execution environment;

a memory including a protected memory area and a non-protected memory area; and

a secure virtual machine monitor (SVMM) to implement the secure execution environment in which a plurality of separate virtual machines are created that operate simultaneously and separately from one another including at least a first virtual machine to implement trusted guest software in the protected memory area and a second virtual machine to implement a non-trusted guest operating system (OS) in the non-protected memory area;

wherein responsive to a command to tear down the secure execution environment, the SVMM causes the processor to exit out of the secure execution mode, tears down the secure execution environment, and instructs the non-trusted guest OS to resume control in the normal execution mode.

24. The system of claim 23, further comprising a virtual machine control structure (VCMS) to store guest state information related to the non-trusted guest operating system (OS) for use in restoring the non-trusted guest OS in the normal execution mode.

25. The system of claim 24, wherein the virtual machine control structure (VCMS) stores a guest OS entry point field to point to a command used for instructing the non-trusted guest OS to resume control at a virtual address and a host entry point field to point to a command to instruct the processor to exit out of a virtual machine execution mode.

26. The system of claim 23, further comprising, the SVMM scrubbing the protected memory associated with the trusted guest software when the secure execution environment is torn down.

27. The system of claim 26, further comprising, the SVMM causing the processor to exit out of a virtual machine extension mode before exiting out of secure execution mode when the secure execution environment is torn down.

28. The system of claim 23, wherein the non-trusted guest operating system (OS) issues the command to tear down the secure execution environment.

29. The system of claim 23, wherein the secure virtual machine monitor (SVMM) issues the command to tear down the secure execution environment.

30. The system of claim 29, wherein the secure virtual machine monitor (SVMM) issues the command to tear down the secure execution environment due to a detected security breach.